PACE
PACE SYSTEMS, INC.

Pace Scheduler
scheduling, simplified

SOLUTIONS since 1983

Pace Scheduler Security

The Pace Scheduler is a cloud based software solution which therefore poses no risk to any internal IT networks. Further, no highly sensitive data is stored anywhere within the Pace Scheduler databases. We do not collect social security numbers, payment information, health information, or external passwords. For all of the data that we do collect, we keep it secure in the following ways:

The Pace Scheduler uses 256-bit secure sockets layer encryption for all communications with our servers. All data is password protected and multiple security and permission layers are enforced at the application level to ensure only the proper users view the data they are entitled to view. Passwords are encrypted using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST. This means even members of the Pace Scheduler development team cannot gain access to a user’s password.

The data is physically stored on the highly secured AWS technology infrastructure. The AWS data center operations have been accredited under ISO 27001, SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II), PCI Level 1, FISMA Moderate, Sarbanes-Oxley (SOX). These centers also provide environmental/disaster safeguards, network security safeguards, and system security safeguards that all comply with industry standards.

Database backups are taken and stored at regular intervals, no less than once per day, and are also stored within the secure AWS technology infrastructure. Every change to your data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state.